Applicant : Taher ELGAMAL et al.
Serial No. : To Be Assigned
Filed : August 3, 2001
Page : 6

Attorney's Docket No.: 06975-193002

REMARKS

Favorable consideration of this application is respectfully requested in view of the above amendments and the following remarks. By this amendment, the specification and Abstract have been editorially amended. The specification now also includes a reference to the parent application. Claims 1-4 have been editorially amended as indicated in the response filed on February 26, 2001, in the parent application. Applicants again submit that no new matter has been added and notice to that effect is solicited. Unless otherwise specifically stated, the claims have been amended to address §112, second paragraph, and form issues, noted by the Applicants, and for no other reason. Currently, claims 1-4 are pending.

In the parent application, claims 1-4 were rejected under 35 USC 101 as allegedly directed to non-statutory subject matter. Applicants respectfully request consideration and withdrawal of this rejection because claims 1-4 are directed to statutory subject matter.

The Examiner asserts that claims 1-4 merely claim nonfunctional descriptive materials stored in a computer-readable medium. Applicants respectfully submit that the Examiner is mistaken. The subject matter of the instant application, as presented in claims 1-4, is "functional descriptive material," which consists of data structures and computer programs, which empart functionality when employed as a computer component. A "data structure" on a computer readable medium provides a physical or logical relationship among data elements designed to support specific data manipulation functions. The subject matter of the instant invention, as functional descriptive material, is not descriptive material *per se* and non-statutory. This is not a mere arrangement of data. When functional descriptive material is recorded on some computer readable medium, it becomes structurally and functionally interrelated to the medium and is statutory since use of technology permits the function of the descriptive material to be realized. MPEP 2100-11.

In the instant case, the claimed computer-readable medium has been encoded with a data structure which defines structural and functional interrelationships between the data structure and the computer software and hardware components which permit the data structure's functionality to be realized, and therefore, the subject matter of claims 1-4 is statutory. In particular, a policy file is stored on the computer medium, as recited in claim 1. Further, claim 1 recites that the

Applicant : Taher ELGAM▓ et al.
Serial No. : To Be Assigned
Filed : August 3, 2001
Page : 7

Attorney's Docket No.: 06975-193002

computer medium includes an attribute portion, a value portion, and a signature portion. Use of this data, the policy file, permits control of the cryptographic capabilities, thus the function of the policy file is realized. Hence, Applicants submit that claims 1-4 are directed to statutory subject matter.

Applicants submit that claims 1-4 recite statutory subject matter, and accordingly, withdrawal of this rejection is respectfully requested.

Attached is a marked-up version of the changes being made by the current amendment.

Applicants respectfully request that all claims be examined and indicated as allowable. Please apply any other charges or credits to Deposit Account No. 06-1050, Ref. No. 06975-193002.

Respectfully submitted,

Date: _August 3, 2001_

Heather Morin
Reg. No. 37,336

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40058981.doc

Applicant : Taher ELGA███ et al.
Serial No. : To Be Assigned
Filed : August 3, 2001
Page : 8

Attorney's Docket No.: 06975-193002

Version with markings to show changes made

In the specification:

Paragraph beginning at page 1, line 3, has been amended as follows:

This application claims a benefit under 35 USC 119(e) of the provisional application filed June 30, 1997, S/N 60/051,307.

This application is a continuation of Application Serial No. 09/940,429, filed September 30, 1997.

Paragraph beginning at page 1, line 4 has been amended as follows:

[Background of the Invention]

Paragraph beginning at page 1, line 5 has been amended as follows:

[Field of the Invention] TECHNICAL FIELD

Paragraph beginning at page 1, lines 6-10 has been amended as follows:

-- **[The present]** This invention relates to cryptography configuration**[.]**, **[M]**more particularly, **[the present invention relates to]** a method and apparatus for controlling the use of cryptography such that products utilizing these controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography. --

Paragraph beginning at page 1, line 12 has been amended as follows:

[Description of the Related Art] BACKGROUND

Applicant : Taher ELGA██████ et al.
Serial No. : To Be Assigned
Filed : August 3, 2001
Page : 9

Att█████y's Docket No.: 06975-193002

Replace the paragraph beginning at page 1, lines 13-30, with the following rewritten paragraph:

-- There are many circumstances where the distribution or the use of encryption software is regulated by the government[s]. In some countries, the strength of encryption that can be exported is regulated without [imposing] any restrictions [upon] on [the] distribution of the encryption software within the country. For example, in the United States, companies are free to distribute any type of encryption software developed within the country for use by Unites States citizens. Furthermore, the United States allows unrestricted importation of encryption technology. However, exporting [of] a certain strength encryption [in] from the United States is regulated. In other countries, such as France, the strength of encryption that can be used, distributed, or imported is tightly regulated.

In the case where [the exporting] exportation of [the] encryption software is restricted, [the] permissible exportable encryption software are usually limited to specific algorithms that use key sizes which are weaker than a particular size. Previously, [the] encryption software has generally been an integral part of a software application. Therefore, to accommodate the varying degrees of [allowed] permitted encryption levels, several versions of the same application are typically created; one version that provides strong encryption by those who are allowed unrestricted use, and one or more versions that use weaker encryption for those customers whose use is restricted. --

Paragraph beginning on page 4, line 22 has been amended as follows:

[SUMMARY OF THE INVENTION] SUMMARY

Paragraph beginning on page 6, line 1 has been amended as follows:

[BRIEF DESCRIPTION OF THE DRAWINGS] DESCRIPTION OF THE DRAWINGS

Paragraph beginning on page 6, lines 2-3 have been amended as follows:

Figure 1 illustrates a block diagram of a system including a policy filter in accordance with [one] an embodiment of the present invention.

Paragraph beginning on page 6, lines 4-5 have been amended as follows:

Figure 2 illustrates a flow chart of the initialization of the policy filter in accordance with [one] an embodiment of the present invention.

Paragraph beginning at page 6, lines 6-7 have been amended as follows:

Figure 3 illustrates a flow chart of the control of capability query through the policy filter in accordance with [one] yet another embodiment of the present invention.

Paragraph beginning at page 6, lines 8-9 have been amended as follows:

Figure 4 illustrates the control of cryptographic operation through the policy filter in accordance with [one] an embodiment of the present invention.

Paragraph beginning at page 6, lines 10-11 have been amended as follows:

Figure 5 illustrates a flow chart of a cryptographic policy module using a cryptographic policy file in accordance with [one] an embodiment of the present invention.

Paragraph beginning at page 6, lines 12-13 have been amended as follows:

Figure 6 illustrates a block diagram of a system including a policy file and module in accordance with [one] an embodiment of the present invention.

Paragraph beginning at page 6, line 15 has been amended as follows:

Applicant : Taher ELGA●●●● et al.
Serial No. : To Be Assigned
Filed : August 3, 2001
Page : 11

Attorney's Docket No.: 06975-193002

[DETAILED DESCRIPTION OF THE INVENTION] DETAILED

DESCRIPTION

Paragraph beginning at page 6, lines 16-17 have been amended as follows:

Figure 1 illustrates a block diagram of a system including policy filters in accordance with [one] an embodiment of the present invention.

Paragraph beginning at page 15, lines 26-29 have been amended as follows:

Although the invention has been described in connection with specific [preferred] embodiments, it should be understood that the invention as claimed should not be unduly limited to such specific embodiments.

In the claims:

Claims 5-30 have been cancelled.

Claims 1-4 have been amended as follows:

1.   A computer readable medium having stored therein a policy file for controlling cryptographic functions of an application program, the computer readable medium comprising:

an attribute portion that [hold] holds a plurality of cryptographic policy attributes, each cryptographic policy [attributes] attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values, each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of [said] the attribute portion and [said] the value portion.

2.   The medium of claim 1, wherein **[said]** the plurality of cryptographic policy attributes includes cryptographic capabilities of **[said]** the application program in a country where **[said]** the application program is said to be executed.

3.   The medium of claim 1, wherein each of **[said]** the attribute values is a data string, an integer number, or a truth expression, **[said]** the truth expression including one of a true flag, a false flag, and a conditional flag.

4.   The medium of claim 1, wherein **[said]** the signature portion includes a digital signature and a chain of certificates, **[wherein said]** the digital signature **[includes]** including a certificate indicative of the origin of **[said]** the digital signature, and **[further, wherein said]** the chain of certificates is indicative of the validity of **[said]** the digital signature.